SIMONT
BRAUN

DIGITAL FINANCE

2019, THE YEAR OF TRUTH FOR OPEN BANKING (RTS - SCA)

JANUARY 2019

INTRODUCTION

In the world of Payments and FinTech, PSD2 has been a hot topic for several years now. Last year was already a crucial year with the transposition deadline of this directive scheduled for 13 January 2018. This transposition gave rise to significant (and by now very well-known) changes such as the introduction of regulation on Account Information Services Providers (AISPs) and Payment Initiation Services Provers (PISPs), commonly referred to as Third Party Payment Service Providers (TPPs)[1].

The most important promise of PSD2, i.e. the instalment of an actual 'open banking' payment culture in Europe, was, however, not yet realised by this 2018 implementation.

By 'open banking' is meant the (forced) sharing of payment account data by so-called account servicing payment service providers (ASPSPs) with other service providers such as TPPs. These ASPSPs are very often banks[2] who will be obliged -without any contractual relationship- to open up their account data, for (usually) FinTech companies to build services around them.

This open banking principle will only go live with the entry into force of the Regulated Technical Standards 2018/389 of 27 November 2017 on Strong Customer Authentication (RTS SCA), scheduled for 14 September 2019.

PREPARE FOR OPEN BANKING

Prior to the entry into force of the RTS SCA, all ASPSPs (basically the banks) need to develop and implement technical solutions that will allow this open banking to take place in a secure and controlled manner. According to the RTS SCA, this should be done by putting in place a so-called 'dedicated interface' (which is, in practice, an Application Programming Interface or 'API'), although also a fall back solution (or 'contingency mechanism') must be foreseen, whereby the TPPs can access the data through the interface used for the authentication of and the communication with the ASPSP's payment service users. In other words: in case the API provided by a bank does not work properly, the TPPs could still access the data through the web-banking service this bank uses itself with its customers. This last technique is often referred to as 'screen-scraping' which is rather controversial since many banks claim this screen-scraping to pose significant security risks, as it implies that their clients need to share their security credentials (login and password) with third parties (TPPs).

The screen-scraping contingency mechanism, as proposed in the RTS, does, however, impose that measures are in place so that banks know at all times who is accessing the data (i.e. either their own customer or a TPP on behalf of this customer).

[1] Please click here the for more information on these acronyms.

[2] Please also note that FinTech companies such as payment and e-money institutions can be subject to this.

This is opposed to the classic/contested way of screen-scraping where banks were under the impression that a client was logging in to their web-banking service, while in reality a TPP was accessing the data with the client's consent (and passwords).

14 MARCH 2019 – INTERMEDIARY DEADLINE

Banks that want to avoid this screen-scraping technique, even only as a fall back solution, are however given a way out by the RTS SCA. But they will need to hurry.

According to article 33(6) of the RTS SCA, ASPSPs such as banks can be exempted from having to provide a contingency mechanism (screen scraping solution) under the condition that their dedicated interface solution (API) is available for testing by TPPs no later than 6 months before the entry into force of the RTS SCA, this means that banks should have their API ready for testing by 14 March 2019.

Industry experts believe this 14 March deadline to be too short for most banks to have a performing API in place since this implies also the provision of testing facilities and technical documents for the TPPs and the supervisors. As a result, those institutions will also have to deliver a screen-scraping based fall back solution (with identification function) by September 2019, which risks to slow them down even more in their API development.

THE RTS AREN'T TECHNICAL ENOUGH…

Regulatory Technical Standards (RTS) are level 2 legislative measures as opposed to the PSD2 itself which is a level 1 legislative act in accordance with the *Lamfalussy* regulatory process for financial services[3]. Level 1 legislation such as the PSD2 is supposed only to set out general framework principles that need further technical implementation (through the level 2 RTS).

Part of the problem here is that the RTS SCA only cover so-called legal-technical aspects and do not impose any operational-technical standards. Chapter V on common and secure open standards of communication of the RTS SCA provides general requirements for communication and set out theoretical requirements for the common and secure open standards of communication. In practice, however, all of this is still very high level from a pure operational-technical point of view.

The RTS only impose certain requirements and finalities on the dedicated interface and the contingency matters without indicating how these results should be obtained. Although it is logic for a legislator not to impose industry standards, this could in practice, without further guidance, lead to as many different interfaces and systems as there are banks in Europe. Certain organisations such as 'Open Banking' in the UK and the 'Berlin Group' on the continent are trying to work out some sort of harmonisation throughout the sector, but do not involve all market participants which certainly poses a threat in terms of competition. There is also a concern that individual member states / supervisors will handle things differently and be either more or either less pragmatic in assessing whether certain requirements are met. Such an approach is potentially harmful since financial services are very often offered on a cross-border basis and industry players will want to avoid local adaptations to their systems.

[3] This process is entailed to provide more convergence in the national implementations and should lead to more consistent interpretation. It has been applied for major financial regulations such as MiFID, the Prospectus Regulation, Market Abuse Directive etc.

MANY QUESTIONS REMAIN UNSOLVED

Next to this, many other questions remain unsolved. What will happen with those banks that do not have an API (and potentially also no fall back solution) in place by 14 September 2019? They will for sure be in breach of the law, but how will supervisors handle this concretely?

What about the large numbers of very small (often private) banks throughout Europe that are also subject to these rules and are facing high investment and development costs to put technical solutions in place, that are similar to those of large retail banks? We see that in this respect, the market has started developing a tendency towards the pooling of smaller players, but a lot remains unclear.

As generally known, the PSD2 rules (and thus also the open banking principle) only concern payment accounts. The Luxembourg based CJEU recently ruled that saving accounts do not qualify as payment accounts and therefore data related to such accounts does not fall under the open banking rules[4]. Banks and TPPs could still contractually decide to open this up to other data (for example on saving and security accounts). However, this could lead to situations where certain data shared through the same API falls under the PSD2 liability scheme (i.e. payment account data), while other data is not covered by this protection (i.e. data on saving and security accounts).

CONCLUSION

An interesting year lies ahead of us, but it is clear that all market participants (banks, TPPs but also supervisors) struggle with the implementation of the open banking principles. Nowadays, financial institutions are all focussing on the near future Brexit obstacle, but will soon be forced to shift, or at least divide their attention in order to tackle this highly topical issue.

* * *

For more information, please contact ***Simont Braun's Digital Finance Team*** *(digitalfinance@simontbraun.eu).*

[4] *Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG* (Case C 191/17) (4 October 2018)